

| (51) Int.Cl. ⁷ | 識別記号 | F I | テ-コ-ト (参考) |
|--------------------------------------|-------|---------------|-------------------|
| G 0 6 K 19/10 | | G 0 6 F 12/14 | 3 1 0 H 5 B 0 1 7 |
| G 0 6 F 12/14 | 3 1 0 | | 3 2 0 B 5 B 0 3 5 |
| | 3 2 0 | | 3 2 0 F 5 B 0 5 8 |
| G 0 6 K 17/00 | | G 0 6 K 17/00 | T 5 J 1 0 4 |
| | | G 0 9 C 1/00 | 6 4 0 E |
| 審査請求 未請求 請求項の数12 O L (全 27 頁) 最終頁に続く | | | |

(21) 出願番号 特願2002-346019(P2002-346019)
 (62) 分割の表示 特願平11-374788の分割
 (22) 出願日 平成11年12月28日 (1999. 12. 28)
 (31) 優先権主張番号 特願平11-119441
 (32) 優先日 平成11年4月27日 (1999. 4. 27)
 (33) 優先権主張国 日本 (J P)

(71) 出願人 000005821
 松下電器産業株式会社
 大阪府門真市大字門真1006番地
 (72) 発明者 廣田 照人
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内
 (72) 発明者 館林 誠
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内
 (74) 代理人 100090446
 弁理士 中島 司朗

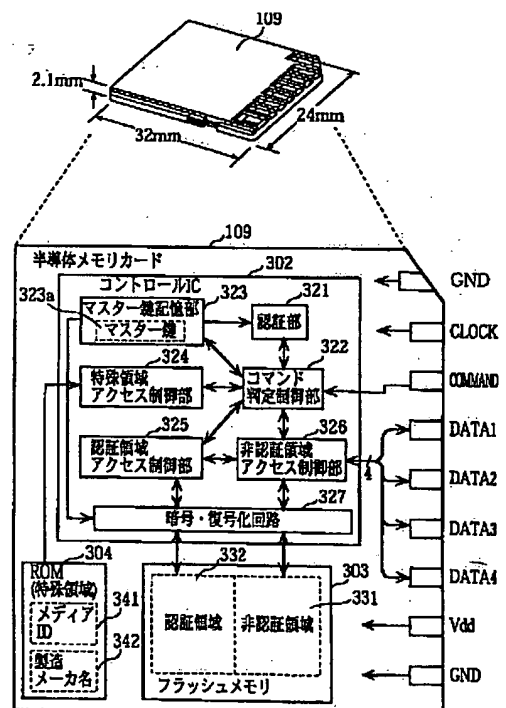
最終頁に続く

(54) 【発明の名称】 半導体メモリカード及び読み出し装置

(57) 【要約】

【課題】 デジタル著作物の記憶媒体として用いることが可能であり、かつ、著作権保護が必要とされない一般的なコンピュータデータ (非著作物) の記憶媒体としても用いることが可能な半導体メモリカードを提供する。

【解決手段】 コントロールIC 302とフラッシュメモリ 303とROM 304とからなり、ROM 304は、このカードに固有のメディアID 341等を保持し、フラッシュメモリ 303は、外部機器の認証に成功した場合にのみその外部機器にアクセスを許可する認証領域 332と認証の結果に拘わらずアクセスを許可する非認証領域 331とを有し、コントロールIC 302は、外部機器による認証領域 332及び非認証領域 331へのアクセスを制御する制御部 325、326及び外部機器との相互認証を実行する認証部 321等を有する。



【特許請求の範囲】

【請求項1】 電子機器に着脱可能な半導体メモリカードであって、
書き換え可能な不揮発メモリと、
前記不揮発メモリ内の予め定められた2つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路と、
前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備え、
前記制御回路は、
前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御部と、
前記電子機器の正当性を検証するために前記電子機器の認証を試みる認証部と、
前記認証部が認証に成功した場合にだけ前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御部とを有し、
前記認証領域と前記非認証領域は、前記不揮発性メモリ内の一定サイズの連続した記憶領域を2分して得られる各領域に割り当てられ、
前記領域サイズ変更回路は、
前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、
前記非認証領域における論理アドレスと物理アドレスとの対応を示す非認証領域変換テーブルと、
前記電子機器からの命令に従って前記認証領域変換テーブル及び前記非認証領域変換テーブルを変更する変換テーブル変更部とを有し、
前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、
前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、
前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を2分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、
前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、
前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられていることを特徴とする半導体メモリカード。

【請求項2】 前記認証部は、認証の結果を反映した鍵データを生成し、
前記認証領域アクセス制御部は、前記電子機器から送られてくる暗号化された命令を前記認証部が生成した鍵データで復号し、復号された命令に従って前記認証領域へのアクセスを制御することを特徴とする請求項1記載の半導体メモリカード。

【請求項3】 前記認証部は、前記電子機器とチャレンジ・レスポンス型の相互認証を行い、前記電子機器の正当性を検証するために前記電子機器に送信したチャレンジデータと自己の正当性を証明するために生成したレスポンスデータとから前記鍵データを生成することを特徴とする請求項2記載の半導体メモリカード。

【請求項4】 前記電子機器から送られてくる暗号化された命令は、前記認証領域へのアクセスの種別を特定する暗号化されていないタグ部と、アクセスする領域を特定する暗号化されたアドレス部とからなり、
前記認証部は、前記鍵データを用いて、前記命令のアドレス部を復号し、復号されたアドレスによって特定される領域に対して、前記命令のタグ部によって特定される種別のアクセスを実行制御することを特徴とする請求項3記載の半導体メモリカード。

【請求項5】 前記半導体メモリカードはさらに、他の半導体メモリカードと区別して自己を特定することが可能な固有の識別データを予め記憶する識別データ記憶回路を備え、
前記認証部は、前記識別データ記憶回路に格納された識別データを用いて相互認証を行い、前記識別データに依存させて前記鍵データを生成することを特徴とする請求項4記載の半導体メモリカード。

【請求項6】 前記半導体メモリカードはさらに、予めデータが格納された読み出し専用のメモリ回路を備えることを特徴とする請求項1記載の半導体メモリカード。

【請求項7】 前記認証領域及び前記非認証領域は、前記電子機器にとって読み書き可能な記憶領域と読み出し専用の記憶領域とからなり、
前記制御回路はさらに、前記電子機器が前記不揮発メモリにデータを書き込むためのアクセスをする度に乱数を発生する乱数発生器を有し、
前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記乱数を用いて前記データを暗号化し、得られた暗号化データを前記読み書き可能な記憶領域に書き込むとともに、前記乱数を前記暗号化データに対応づけられた前記読み出し専用の記憶領域に書き込むことを特徴とする請求項1記載の半導体メモリカード。

【請求項8】 前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有することを特徴とする請求項1記載の半導体メモリカード。

【請求項9】 前記不揮発メモリは、フラッシュメモリであり、
前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記非認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有することを特徴とする請求項1記載の半導体メモリカード。

【請求項10】 前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、

前記制御回路はさらに、

前記ユーザキーを記憶しておくためのユーザキー記憶部と、

前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、

前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有することを特徴とする請求項1記載の半導体メモリカード。

【請求項11】 請求項1記載の半導体メモリカードに格納されたデジタル著作物を読み出す読み出し装置であって、

前記半導体メモリカードは、非認証領域に、デジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の読み出しを許可する回数が予め格納され、前記読み出し装置は、

前記非認証領域に格納されたデジタル著作物を読み出す際に、前記認証領域に格納された回数を読み出し、その回数によって読み出しが許可されているか否か判断する判断手段と、

許可されている場合にのみ前記非認証領域から前記デジタル著作物を読み出すとともに、読み出した前記回数を減算して前記認証領域に書き戻す再生手段とを備えることを特徴とする読み出し装置。

【請求項12】 請求項1記載の半導体メモリカードに格納されたデジタル著作物を読み出してアナログ信号に再生する読み出し装置であって、

前記半導体メモリカードは、非認証領域に、アナログ信号に再生可能なデジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の前記電子機器によるデジタル出力を許可する回数が予め格納され、前記読み出し装置は、

前記非認証領域に格納されたデジタル著作物を読み出してアナログ信号に再生する再生手段と、

前記認証領域に格納された回数を読み出し、その回数によってデジタル出力が許可されているか否か判断する判断手段と、

許可されている場合にのみ前記デジタル著作物をデジタル信号のまま外部に出力するとともに、読み出した前記回数を減算して前記認証領域に書き戻すデジタル出力手段とを備えることを特徴とする読み出し装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタル著作物等

を記憶するための半導体メモリカード及びその読み出し装置に関し、特に、デジタル著作物の著作権保護に好適な半導体メモリカード及び読み出し装置に関する。

【0002】

【従来の技術】 近年、マルチメディア・ネットワーク技術の発展により、音楽コンテンツ等のデジタル著作物がインターネット等の通信ネットワークを通じて配信されるようになり、自宅に居ながらにして世界中の音楽等に接することが可能となってきた。例えば、パーソナルコンピュータ（以下、「PC」という。）で音楽コンテンツをダウンロードした後、PCに装着された半導体メモリカードに格納しておくことで、必要に応じて音楽を再生し楽しむことができる。また、このようにして音楽コンテンツを格納した半導体メモリカードをPCから取り出して携帯型音楽再生装置に装着しておくことで、歩きながら音楽を聴くこともできる。このような半導体メモリカードは、フラッシュメモリ等の不揮発性で、かつ、大きな記憶容量の半導体メモリを内蔵した小型軽量の便利なカードである。

【0003】 ところで、このような電子音楽配信において、半導体メモリカードにデジタル著作物を記憶する場合、不正なコピーを防止するために、鍵等を用いてコンテンツを暗号化しておく必要がある。また、PC等に標準添付されて広く出回っているファイル管理ソフトウェアによっては他の記憶媒体等にコピーすることができないようにしておく必要もある。

【0004】 このような不正なコピーを防止する方法として、半導体メモリカードへのアクセスを専用のソフトウェアでのみ可能とする方策が考えられる。例えば、PCと半導体メモリカード間での認証が成功した時にのみ半導体メモリカードへのアクセスを許可することとし、専用のソフトウェアがないためにその認証に成功することができない場合には半導体メモリカードへのアクセスが禁止されるところの方法が考えられる。

【0005】

【発明が解決しようとする課題】 しかしながら、PCが半導体メモリカードにアクセスするのに常に専用のソフトウェアが必要とされるのでは、そのような専用のソフトウェアを所有していない不特定のユーザと半導体メモリカードを介して自由にデータ交換し合うことが不可能となってしまう。そのために、フラッシュATAやコンパクトフラッシュ（登録商標）等の従来の半導体メモリカードが有していた利便性、即ち、専用のソフトウェアを必要とすることなくPCに標準添付されているファイル管理ソフトウェアでアクセスすることができるという利便性が得られなくなってしまう。

【0006】 つまり、専用のソフトウェアでのみアクセス可能な半導体メモリカードは、著作権保護の機能を有する点でデジタル著作物の記憶媒体としては適しているが、汎用的な使用が困難であるために一般的なコンピュ

ータシステムにおける補助記憶装置として使用することができないという問題点がある。そこで、本発明は、このような問題点に鑑みてなされたものであり、デジタル著作物の記憶媒体として用いることが可能であり、かつ、著作権保護が必要とされない一般的なコンピュータデータ（非著作物）の記憶媒体としても用いることが可能な半導体メモリカード及びその読み出し装置を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため 10
に、本発明に係る半導体メモリカードは、電子機器に着脱可能な半導体メモリカードであって、書き換え可能な不揮発メモリと、前記不揮発メモリ内の予め定められた 2つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路と、前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備え、前記制御回路は、前記非認証領域への前記電子機器によるアクセスを制御する非 20
認証領域アクセス制御部と、前記電子機器の正当性を検証するために前記電子機器の認証を試みる認証部と、前記認証部が認証に成功した場合にだけ前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御部とを有し、前記認証領域と前記非認証領域は、前記不揮発性メモリ内の一定サイズの連続した記憶領域を 2分して得られる各領域に割り当てられ、前記領域サイズ変更回路は、前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、前記非認証領域における論理アドレスと物理アドレスとの 30
対応を示す非認証領域変換テーブルと、前記電子機器からの命令に従って前記認証領域変換テーブル及び前記認証領域変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を 2分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、前記非認証領域変換テーブルは、論理アドレスの昇順が物理 40
アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられていることを特徴とする。

【0008】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。図1は、通信ネットワークを介して音楽コンテンツ等のデジタル著作物をダウンロードするPCと、そのPCに着脱可能な半導体メモリカード（以下、単に「メモリカード」という。）の外観を 50

示す図である。

【0009】PC102は、ディスプレイ103、キーボード104及びスピーカ106等を備え、内蔵するモデムによって通信回線101に接続されている。そして、このPC102が有するPCMCIA等のカードスロット（メモリカードライタ挿入口105）にはメモリカードライタ107が挿入されている。メモリカードライタ107は、PC102とメモリカード109とを電氣的に接続するアダプタであり、そのメモリカード挿入口108にメモリカード109が装着されている。

【0010】このようなシステムを用いることによって、ユーザは、以下の手順を経ることで、インターネット上にあるコンテンツプロバイダが提供する音楽データを取得することができる。まず、ユーザは、所望の音楽コンテンツを、通信回線101を通じて、PC102内部のハードディスクにダウンロードする。音楽データは暗号化されており、そのままではPC102では再生することはできない。

【0011】再生するためには、ダウンロード元のコンテンツプロバイダへクレジットカード等を用いてお金を払っておく必要がある。支払いを済ますと、コンテンツプロバイダよりパスワードと権利情報を入手することができる。パスワードは、暗号化された音楽データを解除するのに必要な鍵データである。権利情報は、PCでの再生可能回数や、メモリカードへの書き込み可能回数、再生可能な期間を示す再生期限等のユーザに許可された再生条件を示す情報である。

【0012】パスワードと権利情報を取得したユーザは、PC102のスピーカ106から音楽を再生出力させる場合には、著作権保護機能が付いた専用のアプリケーションプログラム（以下、このプログラムを単に「アプリケーション」という。）に対して、入手したパスワードをキーボード104から入力する。すると、そのアプリケーションは、権利情報を確認した後に、暗号化された音楽データをパスワードを用いて復号しながらスピーカ106を通じて音声として再生出力する。

【0013】また、権利情報としてメモリカードへの書き込みが許可されている場合には、そのアプリケーションは、暗号化された音楽データ、パスワード、権利情報をメモリカード109に書き込むことができる。図2は、このメモリカード109を記録媒体とする携帯型の録音再生装置（以下、「プレーヤ」という。）201の外観を示す図である。

【0014】プレーヤ201の上面には、液晶表示部203と操作ボタン202が設けられ、手前側面には、メモリカード109を着脱するためのメモリカード挿入口206及びPC102等と接続するためのUSB等の通信ポート213が設けられ、右側面には、アナログ出力端子204、デジタル出力端子205及びアナログ入力 50
端子223等が設けられている。

【0015】プレーヤ201は、メモ리카ード109に格納された音楽データ、パスワード、権利情報に基づいて、再生が許可されている状態にあるならば、その音楽データを読み出して復号した後にアナログ信号に変換し、アナログ出力端子204に接続されたヘッドフォン208を通じて音声として出力したり、再生中の音楽データをデジタルデータのままデジタル出力端子205に出力したりする。

【0016】また、このプレーヤ201は、マイク等を介してアナログ入力端子223から入力されるアナログの音声信号をデジタルデータに変換してメモ리카ード109に記録したり、通信ポート213を介して接続されたPC102と通信することによって、そのPC102によってダウンロードされた音楽データ、パスワード及び権利情報をメモ리카ード109に記録することができる。つまり、このプレーヤ201は、メモ리카ード109への音楽データの記録及びメモ리카ード109に記録された音楽データの再生に関して、図1に示されたPC102及びメモ리카ードライタ107に置き換わる機能を有する。

【0017】図3は、PC102のハードウェア構成を示すブロック図である。PC102は、CPU110、デバイス鍵111aや制御プログラム111b等を予め記憶しているROM111、RAM112、ディスプレイ103、通信回線101と接続するためのモデムポートやプレーヤ201と接続するためのUSB等を備える通信ポート113、キーボード104、内部バス114、メモ리카ード109と内部バス214とを接続するメモ리카ードライタ107、メモ리카ード109から読み出された暗号化音楽データを復号するデスクランブラ1117、復号された音楽データを伸張するMPEG2-AAC (ISO13818-7) に準拠したAACデコーダ118、伸張されたデジタル音楽データをアナログ音声信号に変換するD/Aコンバータ119、スピーカ106及びファイル管理ソフトウェアやアプリケーションを格納しているハードディスク120等から構成される。

【0018】このPC102は、ハードディスク120に格納されたファイル管理ソフトウェアを実行することで、メモ리카ード109をハードディスクのように独立したファイルシステム (ISO9293等) を有する補助記憶装置として用いることができるだけでなく、ハードディスク120に格納された上述の専用アプリケーションを実行することで、通信ポート113のモデム等を介して通信回線101から音楽コンテンツ等をダウンロードしたり、メモ리카ード109との相互認証を行なった後に音楽コンテンツ等をメモ리카ード109に格納したり、メモ리카ード109に格納されている音楽コンテンツ等を読み出してスピーカ106に再生出力したりする。

【0019】なお、ROM111に格納されたデバイス鍵111aは、このPC102に固有の秘密鍵であり、後述するように、相互認証等に用いられる。図4は、プレーヤ201のハードウェア構成を示すブロック図である。プレーヤ201は、CPU210、デバイス鍵211aや制御プログラム211b等を予め記憶しているROM211、RAM212、液晶表示部203、PC102等と接続するためのUSB等の通信ポート213、操作ボタン202、内部バス214、メモ리카ード109と内部バス214とを接続するカードI/F部215、メモ리카ード109との相互認証を実行する認証回路216、メモ리카ード109から読み出された暗号化音楽データを復号するデスクランブラ217、復号された音楽データ伸張するMPEG2-AAC (ISO13818-7) に準拠したAACデコーダ218、伸張されたデジタル音楽データをアナログ音声信号に変換するD/Aコンバータ219、スピーカ224、アナログ入力端子223から入力されたアナログ音楽信号をデジタル音楽データに変換をするA/Dコンバータ221、そのデジタル音楽データをMPEG2-AAC (ISO13818-7) に準拠して圧縮符号化するAACエンコーダ220、圧縮符号化された音楽データを暗号化するスクランブラ222、アナログ出力端子204、デジタル出力端子205及びアナログ入力端子223から構成される。

【0020】このプレーヤ201は、ROM211に格納された制御プログラム211bをRAM212にロードしCPU210に実行させることで、メモ리카ード109に格納されている音楽コンテンツ等を読み出してスピーカ224に再生出力したり、アナログ入力端子223や通信ポート213を経て入力された音楽コンテンツ等をメモ리카ード109に格納したりする。つまり、通常のプレーヤと同様に、個人的に音楽を録音したり再生したりして楽しむことができるだけでなく、PC102によりダウンロードされた電子音楽配信に係る (著作権保護が必要とされる) 音楽コンテンツの記録・再生もできる。

【0021】図5は、メモ리카ード109の外観及びハードウェア構成を示す図である。メモ리카ード109は、何度も繰り返して書き込みが行える書き換え可能な不揮発性メモリを内蔵しており、その記憶容量は64MBであり、外部から3.3Vの電源とクロック信号の供給を受けて動作する。また、メモ리카ード109は、厚さ2.1mm、縦32mm、横24mmの直方体形状で、その側面に書き込み防止スイッチ (ライトプロテクトSW) を有し、9ピンの接続端子によって電氣的に外部機器と接続される。

【0022】このメモ리카ード109は、3つのICチップ (コントロールIC302、フラッシュメモリ303、ROM304) を内蔵している。フラッシュメモリ

303は、一括消去型の書き換え可能な不揮発メモリであり、論理的な記憶領域として、正当な機器であると認証することができた機器だけに対してアクセスを許可する記憶領域である認証領域332と、そのような認証を必要とすることなくアクセスを許可する記憶領域である非認証領域331等を有する。ここでは、認証領域332は、著作権保護に関わる重要なデータを格納するために用いられ、非認証領域331は、一般的なコンピュータシステムにおける補助記憶装置として用いられる。なお、これら2つの記憶領域は、フラッシュメモリ303上の一定のアドレスを境界として区分されている。

【0023】ROM304は、特殊領域と呼ばれる読み出し専用の記憶領域を有し、このメモリカード109に固有の識別情報であるメディアID341やこのメモリカード109の製造メーカー名342等の情報を予め保持している。なお、メディアID341は、他の半導体メモリカードと区別して自己を特定することが可能な固有の識別データであり、ここでは、機器間の相互認証に用いられ、認証領域332への不正なアクセスを防止するために使用される。

【0024】コントロールIC302は、アクティブ素子（論理ゲート等）からなる制御回路であり、認証部321、コマンド判定制御部322、マスター鍵記憶部323、特殊領域アクセス制御部324、認証領域アクセス制御部325、非認証領域アクセス制御部326及び暗号・復号化回路327等を有する。認証部321は、このメモリカード109にアクセスしようとする相手機器とチャレンジ・レスポンス型の相互認証を行う回路であり、乱数発生器や暗号器等を有し、その暗号器と同一の暗号器を相手機器が有しているか否かを検出することによって、相手機器の正当性を認証する。なお、チャレンジ・レスポンス型の相互認証とは、相手機器の正当性を検証するためにチャレンジデータを相手機器に送り、それに対して相手機器において自己の正当性を証明する処理が施こされて生成されたレスポンスデータを相手機器から受け取り、それらチャレンジデータとレスポンスデータとを比較することで相手機器を認証することができるか否かを判断するという認証ステップを、双方の機器が相互に行うことである。

【0025】コマンド判定制御部322は、コマンドピンを介して入力されたコマンド（このメモリカード109への命令）の種類を判定し実行するデコード回路や制御回路からなるコントローラであり、入力されたコマンドの種類に応じて、各種構成要素321～327を制御する。コマンドには、フラッシュメモリ303のデータを読み・書き・消去するコマンドだけでなく、フラッシュメモリ303を制御するためのコマンド（アドレス空間や未消去データに関するコマンド等）も含まれる。

【0026】例えば、データの読み書きに関しては、認証領域332にアクセスするためのコマンド「SecureRe

ad address count」、[SecureWrite address count] や、非認証領域331にアクセスするためのコマンド「Read address count」、[Write address count] 等が定義されている。ここで、「address」は、読み書きの対象となる一連のセクタ群の最初のセクタの番号であり、「count」は、読み書きする合計セクタ数を示す。また、セクタは、メモリカード109に対してデータを読み書きする際の単位であり、ここでは、512バイトである。

10 【0027】マスター鍵記憶部323は、相互認証の際に相手機器が用いたり、フラッシュメモリ303内のデータを保護するために用いられるマスター鍵323aを予め記憶している。特殊領域アクセス制御部324は、特殊領域（ROM304）に格納されたメディアID341等を読み出す回路である。

20 【0028】認証領域アクセス制御部325及び非認証領域アクセス制御部326は、それぞれ、フラッシュメモリ303の認証領域332及び非認証領域331へのデータ書き込み及び読み出しを実行する回路であり、4本のデータピンを介して外部機器（PC102やプレーヤ201等）との間でデータを送受信する。なお、これらアクセス制御部325、326は、内部に1ブロック分のバッファメモリを有し、論理的には（外部機器とのコマンド上でのアクセスは）セクタを単位として入出力するが、フラッシュメモリ303の内容を書き換えるときには、ブロック（32個のセクタ、16Kバイト）を単位として入出力する。具体的には、ある1個のセクタデータを書き換える場合には、フラッシュメモリ303から該当するブロックをバッファメモリに読み出し、そのブロックを一括消去するとともに、バッファメモリ中の該当セクタを書き換えた後に、そのブロックをバッファメモリからフラッシュメモリ303に書き戻す。

30 【0029】暗号・復号化回路327は、認証領域アクセス制御部325及び非認証領域アクセス制御部326による制御の下で、マスター鍵記憶部323に格納されたマスター鍵323aを用いて暗号化及び復号化を行う回路であり、フラッシュメモリ303にデータを書き込む際にそのデータを暗号化して書き込み、フラッシュメモリ303からデータを読み出した際にそのデータを復号化する。これは、不正なユーザがこのメモリカード109を分解してフラッシュメモリ303の内容を直接解析し、認証領域332に格納されたパスワードを盗む等の不正行為を防止するためである。

40 【0030】なお、コントロールIC302は、これら主要な構成要素321～327の他に、クロックピンから供給されるクロック信号に同期した内部クロック信号を生成し各構成要素に供給する同期回路や、揮発性の記憶領域及び不揮発性の記憶領域等を有する。また、特殊領域（ROM304）に格納されている情報の改ざんを防止するために、そのROM304をコントロールIC

302の中に内蔵させたり、それらの情報をフラッシュメモリ303に格納し、外部から書き込みできないように特殊領域アクセス制御部324が制限をかけてもよい。そのときに、暗号・復号化回路327で暗号化したデータを格納することとしてもよい。

【0031】図6は、PC102やプレーヤ201から見たメモリカード109の記憶領域の種類を示す図である。メモリカード109が有する記憶領域は、大きく分けて、特殊領域304と認証領域332と非認証領域331の3つの領域である。特殊領域304は読み出し専用の領域で、この中のデータに対しては、専用コマンドを用いて読み出しを行う。認証領域332は、PC102又はプレーヤ201とメモリカード109との間で認証が成功した時にのみ読み書きができる領域で、この領域へのアクセスについては暗号化されたコマンドを用いる。非認証領域331は、ATAやSCSI等の公開されたコマンドでアクセスできる、即ち、認証せずに読み書きできる領域である。従って、非認証領域331に対しては、フラッシュATAやコンパクトフラッシュ（登録商標）と同じように、PC102上のファイル管理ソフトウェアでデータの読み書きが可能である。

【0032】3つの記憶領域には、以下の情報を格納することとし、これによって、一般的なPCの補助記憶装置として機能と、電子音楽配信に係る音楽データに対する著作権保護の機能とを提供している。つまり、非認証領域331には、著作権保護の対象となる音楽データが暗号化された暗号化コンテンツ426や、著作権保護とは無関係な一般的なデータであるユーザデータ427等が格納される。認証領域332には、非認証領域331に格納された暗号化コンテンツ426を復号するための秘密鍵となる暗号化キー425が格納される。そして、特殊領域304には、認証領域332にアクセスするために必要とされる情報であるメディアID341が格納されている。

【0033】PC102やプレーヤ201は、まず、装着されたメモリカード109の特殊領域304に格納されたメディアID341を読み出し、それを用いて認証領域332に格納された暗号化キー425、権利情報を取り出す。それら暗号化キー425や権利情報によって再生が許可されていれば、非認証領域331にある暗号化コンテンツ426を読み出し、暗号化キー425で復号しながら、再生を行うことができる。

【0034】もし、あるユーザが不正に入手した音楽データだけをPC102等でメモリカード109の非認証領域331に書き込み、そのようなメモリカード109をプレーヤ201に装着して再生しようとしたとする。しかし、そのメモリカード109の非認証領域331に音楽データが格納されているものの、認証領域332に対応する暗号化キー425や権利情報が存在しないために、そのプレーヤ201は、その音楽データを再生する

ことができない。これによって、正規の暗号化キーや権利情報を伴わないで音楽コンテンツだけをメモリカード109に複製しても、その音楽コンテンツは再生されないで、デジタル著作物の不正な複製が防止される。

【0035】図7は、PC102やプレーヤ201がメモリカード109の各領域にアクセスする際の制限やコマンドの形態を示す図であり、(a)は各領域へのアクセスにおけるルールを示し、(b)は各領域のサイズの変更におけるルールを示し、(c)はメモリカード109の領域を示す概念図である。特殊領域304は、読み出し専用の領域であり、認証せずに専用コマンドでアクセスできる。この特殊領域304に格納されたメディアID341は、認証領域332にアクセスするための暗号化コマンドの生成や復号に用いられる。つまり、PC102やプレーヤ201は、このメディアID341を読み出し、これを用いて認証領域332にアクセスするコマンドを暗号化し、メモリカード109に送る。一方、その暗号化コマンドを受けたメモリカード109は、メディアID341を用いて、その暗号化コマンドを復号し、解釈して実行する。

【0036】認証領域332は、PC102やプレーヤ201等のメモリカード109にアクセスする装置とメモリカード109との間で認証が成功した時にのみアクセスが可能となる領域であり、その大きさは(YYYY+1)個のセクタに相当する。つまり、この認証領域332は、論理的には、第0~YYYYのセクタで構成され、物理的には、フラッシュメモリ303の第XXXX~第(XXXX+YYYY)のセクタアドレスを有するセクタから構成される。なお、セクタアドレスとは、フラッシュメモリ303を構成する全てのセクタそれぞれに対してユニークに付された一連の番号のことである。

【0037】非認証領域331は、認証せずにATAやSCSI等の標準コマンドでアクセスすることが可能で、その大きさはXXXX個のセクタに相当する。つまり、この非認証領域331は、論理的にも物理的にも第0~(XXXX-1)のセクタで構成される。なお、フラッシュメモリ303には、認証領域332や非認証領域331に生じた欠陥ブロック（正常に読み書きできない不良の記憶領域を有するブロック）を代替するための交替ブロックの集まりからなる代替ブロック領域501が予め割り当てられることがある。

【0038】また、特殊領域304は認証なしでアクセスできるとしたが、不正なユーザからの解析を防ぐために、認証を行ってからでないとアクセスできないとしてもよいし、特殊領域304にアクセスするコマンドを暗号化してもよい。次に、図7(b)及び(c)を用いて、認証領域332と非認証領域331それぞれの領域サイズを変更する方法について説明する。

【0039】フラッシュメモリ303に設けられる認証領域332と非認証領域331との合計の記憶容量は、

フラッシュメモリ303の全記憶領域から代替ブロック領域501等を除いた固定値、即ち、(XXXX+YYYYY+1)個のセクタ分であるが、それぞれの大きさは、境界アドレスXXXXの値を変更することで、可変となっている。

【0040】領域の大きさを変更するためには、初めに認証を行う。これは、PCのユーザに広く開放されている標準プログラムや不正なアクセスを行うソフト等を用いて簡単に大きさを変更することができないようにするためである。認証を行った後は、領域変更の専用コマンドで、非認証領域331の大きさ(新たなセクタ数XXXXX)をメモリカード109に送る。

【0041】メモリカード109は、その領域変更コマンドを受け取ると、その値XXXXをメモリカード109内の不揮発な作業領域等に保存し、以降のアクセスにおいては、その値を新たな境界アドレスとして、認証領域332及び非認証領域331へのアクセス制御を実行する。つまり、フラッシュメモリ303上の物理的な第0~XXXXのセクタを非認証領域331に割り当てるとともに、第XXXX~(XXXX+YYYY)番目のセクタを認証領域332に割り当てて、そして、そのような新たなメモリマッピングに基づいて、アクセス制御部325及び326は、論理アドレスと物理アドレスとを変換したり、領域を越えるアクセス違反の発生を監視したりする。なお、論理アドレスとは、外部機器からメモリカード109を見た場合の(コマンド上での)データ空間におけるアドレスであり、物理アドレスとは、メモリカード109のフラッシュメモリ303が有するデータ空間におけるアドレスである。

【0042】ここで、もし、境界アドレスを小さくすることにより、認証領域332のサイズを大きくした場合には、変更前との論理的な互換性を維持するために、認証領域332に格納されていた全てのデータを移動させる等の手当てが必要となる。そのためには、例えば、境界アドレスの移動量だけアドレスの下位方向に全データを移動(複写)させ、新たな境界アドレスから始まる論理アドレスに新たな物理アドレスが対応するように対応関係を変更すればよい。これによって、認証領域332に格納されていたデータの論理アドレスを維持したまま、そのデータ空間が拡大される。

【0043】なお、領域変更のための専用コマンドについても、不正なアクセスを防止する観点から、コマンドを暗号化して用いることとしてもよい。図8は、音楽データ等のコンテンツをPC102(及びプレーヤ201)がメモリカード109に書き込む動作を示すフロー図である。ここでは、PC102がメモリカード109へ書き込む場合(S601)を説明する。

【0044】(1) PC102は、デバイス鍵111a等を用いて、メモリカード109の認証部321とチャレンジ・レスポンス型の認証を行い、その認証に成功す

ると、まず、メモリカード109からマスター鍵323aを取り出す(S602)。

(2) 次に、専用コマンドを用いて、メモリカード109の特殊領域304に格納されているメディアID341を取り出す(S603)。

【0045】(3) 続いて、乱数を生成し、その乱数と、いま取り出したマスター鍵323aとメディアID341とから、音楽データを暗号化するためのパスワードを生成する(S604)。このときの乱数は、例えば、上記認証において、メモリカード109に送信したチャレンジデータ(乱数)を暗号化したもの等を用いる。

(4) 得られたパスワードをマスター鍵323aとメディアID341で暗号化し、暗号化キー425として認証領域332に書き込む(S605)。このときには、データ(暗号化キー425)を送信するのに先立ち、認証領域332に書き込むためのコマンドを暗号化してメモリカード109に送信しておく。

【0046】(5) 最後に、音楽データをパスワードで暗号化しながら暗号化コンテンツ426として非認証領域331に格納していく(S606)。図9は、音楽データ等のコンテンツをメモリカード109から読み出してプレーヤ201(及びPC102)で再生する動作を示すフロー図である。ここでは、メモリカード109内の音楽データをプレーヤ201が再生する場合(S701)を説明する。

【0047】(1) プレーヤ201は、デバイス鍵211a等を用いて、メモリカード109の認証部321とチャレンジ・レスポンス型の認証を行い、その認証に成功すると、まず、メモリカード109からマスター鍵323aを取り出す(S702)。

(2) 次に、専用コマンドを用いて、メモリカード109の特殊領域304に格納されているメディアID341を取り出す(S703)。

【0048】(3) 続いて、メモリカード109の認証領域332から音楽データの暗号化キー425を取り出す(S704)。このときには、データ(暗号化キー425)の読み出しに先立ち、認証領域332から読み出すためのコマンドを暗号化してメモリカード109に送信しておく。

(4) 得られた暗号化キー425をマスター鍵323aとメディアID341で復号化し、パスワードを抽出する(S705)。このときの復号化は、図8に示されたステップS605での暗号化の逆変換である。

【0049】(5) 最後に、非認証領域331から暗号化コンテンツ426を読み出し、上記ステップS705で抽出したパスワードで復号しながら音楽を再生していく(S706)。このように、メモリカード109の非認証領域331に格納された音楽データは、認証領域332の暗号化キー425がないと復号することができな

い。従って、たとえ不正に音楽データだけを別のメモ리카ードにコピーしたとしても、その音楽データを正常に再生することができないので、その音楽データの著作権は安全に保護される。

【0050】また、認証に成功した機器だけがメモ리카ードの認証領域へのアクセスが許可されるので、認証に用いられるデバイス鍵や暗号化アルゴリズム等を適切に選択して用いることで、一定の条件を満たした機器だけに対してメモ리카ードの認証領域へのアクセスを許可する等の著作権保護が可能となる。なお、この例では、メモ리카ード109に暗号化コンテンツを記録する際に、その暗号化に用いられたパスワードをマスター鍵とメディアIDで暗号化し、暗号化キーとして認証領域332に格納されたが(S605)、マスター鍵及びメディアIDのいずれかを用いて暗号化することとしてもよい。これによって、暗号の強度が低下する恐れがあるものの、暗号化の簡略化に伴い、メモ리카ード109やプレーヤ201等の回路規模が小さくなるという利点が得られる。

【0051】また、プレーヤ201やPC102は、認証により、メモ리카ード109からマスター鍵323aを取り出したが、予めプレーヤ201やPC102にそのマスター鍵323aを埋め込んでおいてもよいし、マスター鍵323aを暗号化し、暗号化マスター鍵として特殊領域304に格納しておいてもよい。次に、このようなメモ리카ードの認証領域の活用例として、「読み出し回数」を格納した例と、「デジタル出力許可回数」を格納した例を示す。

【0052】図10は、プレーヤ201(及びPC102)がメモ리카ード109の認証領域に格納された読み出し回数812を操作する動作を示すフロー図である。ここでは、メモ리카ード109に格納された読み出し回数812の範囲内でのみ、プレーヤ201が、メモ리카ード109の非認証領域331に格納された音楽データを音声信号に再生することが許可されている場合(S801)について説明する。

【0053】(1) プレーヤ201は、デバイス鍵211a等を用いて、メモ리카ード109の認証部321とチャレンジ・レスポンス型の認証を行い、その認証に成功すると、まず、メモ리카ード109からマスター鍵323aを取り出す(S802)。

(2) 次に、専用コマンドを用いて、メモ리카ード109の特殊領域304に格納されているメディアID341を取り出す(S803)。

【0054】(3) 続いて、メモ리카ード109の認証領域332から音楽データの暗号化キー425を取り出す(S704)。このときには、データ(暗号化キー425)の読み出しに先立ち、認証領域332から読み出すためのコマンドを暗号化してメモ리카ード109に送信しておく。

(4) 次に、メモ리카ード109の認証領域332から読み出し回数812を取り出し、その値を検査する(S804)。その結果、その値が無制限な読み出しを許可する旨の値である場合は、図9に示された手順(S704~S706)と同様の手順に従って、音楽を再生する(S806~S808)。

【0055】(5) 一方、読み出し回数812が0を示す場合は、もはや再生が許可されていないと判定し(S805)、再生処理を終了する(S809)。そうでない場合は、その読み出し回数812を1つ減算し、その結果を認証領域332に書き戻した後に(S805)、上記手順に従って、音楽を再生する(S806~S808)。

【0056】このように、メモ리카ード109の認証領域332に、予め許可された再生回数を指定した読み出し回数812を格納しておくことにより、プレーヤ201による音楽再生の回数をコントロールすることが可能となる。これによって、例えば、レンタルCDやKIOSK端末等によるアナログ再生に適用することが可能となる。

【0057】なお、読み出し回数812に代えて、「読み出し時間」とすることで、音楽コンテンツを再生することが可能な総時間を制限することもできる。また、回数と時間とを組み合わせてもよい。さらに、読み出し回数812は、再生を開始してから10秒等の一定時間を超えて再生され続けた場合にだけ、その回数を減算してもよい。また、読み出し回数812は、不正な改ざんを防ぐために暗号化して格納することとしてもよい。

【0058】図11は、プレーヤ201(及びPC102)がメモ리카ード109の認証領域に格納されたデジタル出力許可回数913を操作する動作を示すフロー図である。ここでは、メモ리카ード109に格納されたデジタル出力許可回数913の範囲内でのみ、プレーヤ201が、メモ리카ード109の非認証領域331に格納された音楽データを読み出してデジタル出力することが許可されている場合(S901)について説明する。

【0059】(1) プレーヤ201は、図9に示された再生の場合(S701~S705)と同様にして、メモ리카ード109と認証を行なった後にマスター鍵323aを取り出し(S902)、メディアID341を取り出し(S903)、暗号化キー425を取り出す(S904)、パスワードを抽出する(S905)。

(2) 次に、メモ리카ード109の認証領域332からデジタル出力許可回数913を取り出し、その値を検査する(S906)。その結果、その値が無制限なデジタル出力を許可する旨の値である場合は、非認証領域331から暗号化コンテンツ426を読み出し、上記ステップS905で抽出したパスワードで復号しながらデジタルな音楽データとしてデジタル出力端子205から出力する(S909)。

【0060】(3) 一方、デジタル出力許可回数913が0を示す場合は、もはやデジタル出力は許可されていないと判定し(S908)、アナログ出力による再生だけを行なう(S908)。つまり、非認証領域331から暗号化コンテンツ426を読み出し、パスワードで復号しながら音楽を再生する(S908)。

(4) 読み出したデジタル出力許可回数913が0ではない一定の制限回数を示す場合は、その回数を1つ減算し、その結果を認証領域332に書き戻した後に(S907)、非認証領域331から暗号化コンテンツ426を読み出し、上記ステップS905で抽出したパスワードで復号しながらデジタルな音楽データとしてデジタル出力端子205から出力する(S909)。

【0061】このように、メモ리카ード109の認証領域332に、予め許可されたデジタル出力の回数を指定したデジタル出力許可回数913を格納しておくことにより、プレーヤ201による音楽データのデジタル出力の回数をコントロールすることが可能となる。これによって、例えば、レンタルCDやKIOSK端末等によるデジタル再生への適用、即ち、メモ리카ードに記憶した音楽データのデジタルダビングを著作権者の了解の元に指定した回数分だけコピーを許可するような運用が実現となる。

【0062】なお、「読み出し回数」の場合と同様に、デジタル出力許可回数913に代えて、「デジタル出力許可時間」とすることで、音楽コンテンツをデジタルデータのまま出力することが可能な総時間を制限することもできる。また、回数と時間とを組み合わせてもよい。さらに、デジタル出力許可回数913は、その出力を開始してから10秒等の一定時間を超えて出力され続けた場合にだけ、その回数を減算してもよい。また、デジタル出力許可回数913は、不正な改ざんを防ぐために暗号化して格納することとしてもよい。

【0063】さらに、著作権者に代金を払い込むことで、著作権者が指定した回数だけデジタル出力許可回数を増やす機能を追加してもよい。次に、このメモ리카ード109の物理的なデータ構造(セクタ及びECCブロックの構造)について説明する。このメモ리카ード109では、フラッシュメモリ303に格納されたデータのバックアップと復元に伴う不正行為やデータの改ざんに伴う不正行為等を防止するのに好適なデータ構造が採用されている。つまり、上述のような「読み出し回数」や「デジタル出力許可回数」を認証領域332に格納し、それら行為を実行する度にカウントダウンしていく方式では、次のような攻撃を受ける可能性がある。

【0064】つまり、フラッシュメモリ303全体の記憶データを外部の補助記憶装置等にバックアップしておいた後に音楽再生を繰り返す、それら回数が0となった時点でバックアップデータを復元することにより、再び音楽再生を繰り返したり、「読み出し回数」そのものを

改ざんすることで、不正に音楽再生を繰り返すことが考えられる。従って、そのような行為を防止する手当てが必要となる。

【0065】図12は、メモ리카ード109の認証領域332及び非認証領域331に共通のデータ構造と、そのデータ構造に対応した読み書き処理のフローとを示す図である。ここでは、コントロールIC302の認証部321等有する乱数発生器1003が発生するカウンタ値が時変の鍵として利用される。

【0066】フラッシュメモリ303には、512バイトのセクタ1004ごとに、16バイトの拡張領域1005が割り当てられる。各セクタは、カウンタ値で暗号化されたデータが格納される。拡張領域1005は、対応するセクタに格納されている暗号化データの誤り訂正符号を格納するための8バイトのECCデータ1006と、その暗号化データの生成に用いられたカウンタ値を格納するための8バイトの時変領域1007とからなる。

【0067】なお、論理的に(ユーザに開放されたコマンド等を用いて)アクセス可能な領域はセクタ1004だけであり、拡張領域1005は、物理的に(メモ리카ードを読み書きする装置による制御として)のみアクセス可能な領域である。このようなデータ構造とすることで、コマンド等を用いてセクタデータだけが改ざんされても、時変領域1007の内容は変更されることがないので、それらの整合性を利用することで、不正な改ざんを防止することができる。

【0068】具体的には、PC102やプレーヤ201は、セクタ1004ごとに、以下の手順に従って、フラッシュメモリ303の認証領域332や非認証領域331にデータを格納したり、読み出したりする。ここでは、まず、PC102がメモ리카ード109にデータを書き込む場合(S1001)の手順を説明する。

(1) PC102は、メモ리카ード109に対してカウンタ値の発行を要求する。すると、メモ리카ード109内のコントロールIC302は、内部の乱数発生器1003で乱数を発生し(S1005)、その乱数をカウンタ値としてPC102等へ送る(S1002)。

【0069】(2) 取得したカウンタ値と、既に取得しているマスター鍵323a及びメディアID341とからパスワードを生成する(S1003)。

(3) 書き込むべき1セクタ分のデータをパスワードで暗号化しながら、メモ리카ード109に送る(S1004)。このとき、書き込むべきセクタを指定する情報や、暗号化に用いたカウンタ値も一緒に送る

(4) メモ리카ード109は、受け取った暗号化データを、指定されたセクタ1004に書き込む(S1006)。

【0070】(5) その暗号化データからECCを計算し、上記セクタに対応する拡張領域1005に、ECC

データ1006として書き込む(S1007)。

(6) 続いて、上記暗号化データとともに受け取ったカウンタ値を時変領域1007に書き込む(S1008)。

次に、PC102がメモ리카ード109からデータを読み出す場合(S1011)の手順を説明する。

【0071】(1) PC102は、メモ리카ード109に対して、セクタを指定するとともにデータの読み出しを要求する。すると、メモ리카ード109は、まず、指定されたセクタ1004の暗号化データだけを読み出して 10 PC102に出力し(S1016)、PC102は、その暗号化データを受け取る(S1012)。

(2) 次に、メモ리카ード109は、指定されたセクタ1004に対応する拡張領域1005の時変領域1007に格納されたカウンタ値を読み出してPC102に出力し(S1017)、PC102は、そのカウンタ値を受け取る(S1013)。

【0072】(3) 読み出したカウンタ値と、既已取得しているマスター鍵323a及びメディアID341とからパスワードを生成する(S1014)。

(4) そのパスワードを用いて、暗号化データを復号する(S1015)。

ここで、もし、不正な改ざん等により、セクタ1004のデータが変更されている場合には、時変領域1007から読み出されたカウンタ値との不整合が生じ、元のデータに復元されない。

【0073】このように、フラッシュメモリ303内に、ユーザからは見えない(アクセスできない)隠し領域としての時変領域1007を設け、そこに格納されたカウンタ値に依存したパスワードでデータを暗号化し 30 格納することで、不正なユーザによるデータの改ざんを防止することができる。なお、ここでは、時変領域1007は、ECCを格納するための拡張領域1005としたが、メモ리카ードの外部から書き換えができない領域であれば、フラッシュメモリ303内の他の領域に設けてもよい。

【0074】また、カウンタ値は、乱数であったが、刻々と変化する時刻等のタイマ値としたり、フラッシュメモリ303への書き込み回数を示す値としてもよい。次に、フラッシュメモリ303の論理アドレスと物理 40 アドレスとの対応づけについて、好ましい例を説明する。図13は、論理アドレスと物理アドレスとの対応を変更する様子を示す図であり、(a)は変更前の対応関係、(b)は変更後の対応関係、(c)は(a)に対応する変換テーブル1101、(d)は(b)に対応する変換テーブル1101を示す。

【0075】ここで、変換テーブル1101は、全ての論理アドレス(ここでは、論理ブロックの番号)と各論理アドレスに対応する物理アドレス(ここでは、フラッシュメモリ303を構成する物理ブロックの番号)とを 50

組にして記憶するテーブルであり、コントロールIC302内の不揮発な記憶領域等に保存され、認証領域アクセス制御部325や非認証領域アクセス制御部326によって論理アドレスを物理アドレスに変換する際等において参照される。

【0076】メモ리카ード109にアクセスする機器は、メモ리카ード109中の物理的に存在するすべてのデータ空間(フラッシュメモリ303を構成する全ての物理ブロック)にデータを書き込めるのではなく、論理アドレスによって特定できる論理的なデータ空間(論理ブロック)にのみデータを書き込むことができる。この理由の一つは、フラッシュメモリ303の一部が破損し読み書きが行えなくなった場合に、その領域を置き換えるための代替領域を確保しておかなければならないからである。そして、そのような欠陥ブロックを代替領域中のブロックと置き換えた場合であっても、その対応づけの変更を変換テーブルに反映しておくことで、複数の連続する物理ブロックからなるファイルの論理的な連続性は維持されるので、外部機器に対しては破損が生じなかったように見せかけることができる。

【0077】ところが、複数のブロックからなるファイル等をメモ리카ード109に格納したり、削除したりすることを繰り返していると、論理ブロックのフラグメンテーションが増大する。つまり、図13(a)に示されるように、同一のファイルfile1を構成する論理ブロックであるにも拘わらず、それらの論理アドレスが不連続となってしまう。

【0078】これでは、例えば、音楽データをメモ리카ード109に格納しようとしたときに、メモ리카ード109の論理的な連続領域に書けないので、各ブロック毎に書き込みコマンド「Write address count」を発行する必要があり、書き込み速度が低下してしまう。同様に、読み出し動作においても、1曲を構成する音楽データであるにも拘わらず、各ブロック毎に読み出しコマンド「Read address count」を発行する必要があり、音楽データのリアルタイム再生が困難となってしまう。

【0079】この問題を解決する方法として、このメモ리카ード109のコントロールIC302は、外部機器からのコマンドに基づいて、変換テーブル1101を書き換える機能を有する。具体的には、コントロールIC302のコマンド判定制御部322は、変換テーブル1101を書き換えるための専用コマンドがコマンドピンから入力されると、そのコマンドを解釈し、続いて送られてくるパラメータを用いて変換テーブル1101を書き換える。

【0080】その具体的な動作は、図13に示される通りである。いま、上記専用コマンドが送られてくる前においては、フラッシュメモリ303において、図13

(a)に示されるように、物理アドレス0及び2にファイルfile1を構成するデータが存在し、物理アドレス1

にファイルfile2を構成するデータが存在するとする。そして、変換テーブル1101には、図13(c)に示されるように、物理アドレスと論理アドレスとが一致する内容が保持されているとする。つまり、物理アドレス上と同様に、論理アドレス上においても、ファイルfile2のデータが別のファイルfile1のデータに挟まれて格納されているとする。

【0081】このような状態を解消しようとする外部機器は、フラッシュメモリ303に対して、特定のファイルfile1の連続性を確保する旨を示す上記専用コマンド及びパラメータを送る。すると、メモリカード109の

コマンド判定制御部322は、その専用コマンド及びパラメータに従って、変換テーブル1101を図13(d)に示される内容に書き換える。つまり、フラッシュメモリ303の論理及び物理アドレスの対応関係は、図13(b)に示されるように変更される。

【0082】図13(b)に示された関係図から分かるように、物理ブロックの配置は変化していないにも拘わらず、ファイルfile1を構成する2つの論理ブロックが連続するように再配置されている。これによって、その外部機器は、次のアクセス以降においては、それまでもより高速にファイルfile1にアクセスすることが可能となる。

【0083】以上のような変換テーブル1101の変更は、論理ブロックのフラグメンテーションを解消するためだけでなく、フラッシュメモリ303の認証領域332と非認証領域331それぞれのサイズを変更する場合にも用いられる。このときには、サイズを小さくする領域の物理ブロックがサイズを大きくする領域の物理ブロックとして割り当てられるように変換テーブル1101を書き換えるだけで済むので、高速な領域変更が可能となる。

【0084】次に、このメモリカード109が有する未消去ブロックに関する機能、具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行なわれ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用される(書き込まれる)前に一括消去が必要とされる物理ブロックである。

【0085】また、未消去リストコマンドとは、コマンド判定制御部322が解釈及び実行可能なコマンドのひとつであり、その時点におけるフラッシュメモリ303に存在する全ての未消去ブロックの番号の一覧を取得するためのコマンドである。メモリカード109に使用されているフラッシュメモリ303は、書き込みを行う前にブロック単位での一括消去が必要とされるが、その消去処理は書き込み時間の半分近くを占めるため、予め消去しておいた方がより高速に書き込むことができる。そ

こで、このメモリカード109は、その便宜を図るために、未消去リストコマンドと消去コマンドを外部機器に提供している。

【0086】いま、フラッシュメモリ303は、図14(a)に示されるような論理ブロック及び物理ブロックの使用状態とする。ここでは、論理ブロック0~2が使用中であり、物理ブロック0~2、4及び5が未消去ブロックとなっている。この状態においては、コマンド判定制御部322内に保持されている未消去リスト1203は、図14(b)に示される内容となっている。ここで、未消去リスト1203は、フラッシュメモリ303を構成する全ての物理ブロックに対応するエントリーからなる記憶テーブルであり、コマンド判定制御部322による制御の下で、対応する物理ブロックの消去状態に応じた値(消去済みの場合は“0”、未消去の場合は“1”)が保持される。

【0087】図14(c)は、このような状態においてPC102やプレーヤ201が未消去リストコマンドと消去コマンドを用いて事前にブロックを消去する場合の動作を示すフロー図である。なお、フラッシュメモリ303には、図14(d)に示されるように、論理ブロックの使用状態を示すFAT(File Allocation Table)等のテーブルが格納されているものとする。

【0088】PC102やプレーヤ201等の外部機器は、例えば、メモリカード109へのアクセスが発生していないアイドル時間において、このメモリカード109に対して未消去リストコマンドを発行する(S1201)。そのコマンドを受け取ったメモリカード109のコマンド判定制御部322は、内部に有する未消去リスト1203を参照することで、状態値1が登録されている物理ブロックの番号0~2、4及び5を特定し、その外部機器に返す。

【0089】続いて、外部機器は、フラッシュメモリ303に格納された図14(d)に示される論理ブロックの使用状態を示すテーブルを参照することで、論理的に使用されていないブロックを特定する(ステップS1202)。そして、上記2つのステップS1201及びS1202で取得した情報に基づいて、消去可能なブロック、即ち、論理的に不使用で、かつ、物理的に未消去なブロック(ここでは、物理ブロック4と5)を特定した後(ステップS1203)、メモリカード109に対して、それらブロック4と5の番号を指定した消去コマンドを発行する(ステップS1204)。そのコマンドを受信したメモリカード109のコマンド判定制御部322は、アクセス制御部325、326に指示を出す等により、指定された物理ブロック4と5を一括消去する。

【0090】これによって、もし、その物理ブロック4と5への書き込みが発生した場合には、その物理ブロックに対する消去処理は不要となるので、高速な書き込み

が可能となる。次に、このメモリカード109が有する個人データの保護に関する機能、具体的には、メモリカード109が外部機器を認証する際にその外部機器を使用するユーザの個人データを必要とする場合における個人データの保護機能について説明する。ここで、個人データとは、そのユーザを一意に識別するためのデータであって、メモリカード109の認証領域332へのアクセスが許可された正規のユーザとしてメモリカード109に識別させるためのデータである。

【0091】このような場合において、認証領域332へのアクセスの度にユーザに対して繰り返し個人データを入力することを要求したり、その個人データを認証領域332に格納することとしたのでは、不正者によって盗聴されたり、認証領域332にアクセスする権限を有する他のユーザによって見られたりする不都合がある。

【0092】これを防止するために、音楽データと同様に、個人データについても、個人が設定したパスワードで暗号化してから格納するという方法が考えられる。しかしながら、パスワードを設定した場合には、その個人データを見るたびにパスワードを入力しなければならず、手続が面倒であり、その管理も必要となる。そこで、このメモリカード109は、不必要に個人データを繰り返し入力することを回避する機能を有する。

【0093】図15は、認証のためのプレーヤ201とメモリカード109間の通信シーケンス及び主要な構成要素を示す図である。なお、本図に示される処理は、主にプレーヤ201の認証回路216及びメモリカード109の認証部321によって実現される。本図に示されるように、プレーヤ201の認証回路216は、暗号化及び復号化等の機能の他に、メモリカード109に保持されたマスター鍵323aと同一の秘密鍵であるマスター鍵1301と、製造番号(s/n)等のプレーヤ201に固有のIDである機器固有ID1302とを予め記憶している。

【0094】また、メモリカード109の認証部321は、暗号化、復号化及び比較等の機能に他に、2つの不揮発な記憶領域である機器固有ID群記憶領域1310とユーザキー記憶領域1311とを有する。機器固有ID群記憶領域1310は、このメモリカード109の認証領域332へのアクセスが許可された全ての機器の機器固有IDを記憶しておくための記憶領域であり、ユーザキー記憶領域1311は、個人データとして機器から送られてきたユーザキーを記憶しておくための記憶領域である。

【0095】具体的な認証手順は、以下の通りである。なお、送受信においては、全てのデータは暗号化されて送信され、受信側で復号される。そして、手順が進む度に、次の手順での暗号化及び復号化に用いられる鍵が生成される。

(1) メモリカード109とプレーヤ201とを接続す

ると、まず、プレーヤ201は、マスター鍵1301を用いて機器固有ID1302を暗号化し、メモリカード109に送る。

【0096】(2) メモリカード109は、受け取った暗号化された機器固有ID1302をマスター鍵323aで復号し、得られた機器固有ID1302が既に機器固有ID群記憶領域1310に格納されているか検査する。

(3) その結果、既に機器固有ID1302が格納されている場合は、認証が成功した旨をプレーヤ201に通知し、一方、機器固有ID1302が格納されていない場合は、プレーヤ201に対しユーザキーを要求する。

【0097】(4) プレーヤ201は、ユーザキーの入力をユーザに促した後に、ユーザから個人データとしてのユーザキーを取得し、そのユーザキーをメモリカード109に送る。

(5) メモリカード109は、送られてきたユーザキーと予めユーザキー記憶領域1311に格納されているものとを比較し、一致している場合、又は、ユーザキー記憶領域1311が空であった場合は、認証が成功した旨をプレーヤ201に通知するとともに、上記ステップ

(3)で獲得した機器固有ID1302を機器固有ID群記憶領域1310へ格納する。

【0098】これによって、ユーザが所有する機器とメモリカード109とを初めて接続した場合は個人データ(ユーザキー)の入力が必要とされるが、2回目以降においては、その機器の機器固有IDが用いられて自動的に認証が成功するので、再び、個人データの入力を要求されることはない。次に、本メモリカード109とPC102やプレーヤ201等の外部機器との認証プロトコルの変形例について、図16及び図17を用いて説明する。

【0099】図16は、変形例に係るメモリカード109と外部機器(ここでは、プレーヤ201)との認証手順を示す通信シーケンス図である。ここでの処理は、主に、変形例に係るプレーヤ201の認証回路216、PC102の制御プログラム111b及びメモリカード109の認証部321によって実現される。また、メモリカード109のマスター鍵記憶部323には、暗号化されたマスター鍵(暗号化マスター鍵323b)が格納されており、特殊領域304には、メディアID341に加えて、そのメディアID341を暗号化して得られるセキュアメディアID343も格納されているものとする。

【0100】まず、プレーヤ201は、メモリカード109にコマンドを発することで、メモリカード109のマスター鍵323bを取り出し、デバイス鍵211aで復号する。ここでの復号アルゴリズムは、メモリカード109に格納されている暗号化マスター鍵323bが生成された際に用いられた暗号アルゴリズムに対応する。

従って、このプレーヤ201が有するデバイス鍵211aが予定されたもの(正規のもの)であれば、この復号によって元のマスター鍵に復元される。

【0101】続いて、プレーヤ201は、メモリカード109にコマンドを発することで、メモリカード109のメディアID341を取り出し、復元された上記マスター鍵で暗号化する。ここでの暗号アルゴリズムは、メモリカード109に格納されているセキュアメディアID343が生成された際に用いられた暗号アルゴリズムと同一である。従って、ここでの暗号化によって、メモリカード109が有するセキュアメディアID343と同一のセキュアメディアIDが得られる。

【0102】続いて、それらセキュアメディアIDそれぞれを用いて、プレーヤ201とメモリカード109は、相互認証を行なう。その結果、いずれの機器においても、相手機器の認証に成功したか否かを示す(OK/NG)情報と、その認証結果に依存して定まる時変の鍵であるセキュア鍵とが生成される。このセキュア鍵は、双方の機器201及び109が認証に成功した場合にのみ一致し、かつ、相互認証を繰り返す度に変動する性質を有する。

【0103】続いて、相互認証に成功すると、プレーヤ201は、メモリカード109の認証領域332にアクセスするためのコマンドを生成する。具体的には、例えば、認証領域332からデータを読み出す場合であれば、そのコマンド「SecureReadaddress count」のパラメータ(24ビット長のアドレス「address」と8ビット長のカウンタ「count」)をセキュア鍵で暗号化し、得られた暗号化パラメータと、そのコマンドのタグ(コマンドの種類「SecureRead」を示す6ビット長のコード)とを連結して得られる暗号化コマンドをメモリカード109に送る。

【0104】暗号化コマンドを受け取ったメモリカード109は、そのタグからコマンドの種類を判定する。ここでは、認証領域332からの読み出しコマンド「SecureRead」であると判定する。その結果、認証領域332へのアクセスコマンドであると判定した場合には、そのコマンドに含まれていたパラメータを、相互認証で得られたセキュア鍵で復号する。ここでの、復号アルゴリズムは、プレーヤ201において暗号化コマンドを生成する際に用いられた暗号アルゴリズムに対応するので、相互認証が成功していれば、即ち、双方の機器で用いられるセキュア鍵が一致していれば、この復号によって得られるパラメータは、プレーヤ201で用いられた元のパラメータに等しくなる。

【0105】そして、メモリカード109は、復号されたパラメータによって特定されるセクタに格納された暗号化キー425を認証領域332から読み出し、それをセキュア鍵により暗号化しプレーヤ201に送信する。プレーヤ201は、送られてきたデータを、相互認証で

得られたセキュア鍵を用いて復号する。ここでの、復号アルゴリズムは、メモリカード109において暗号化キー425の暗号化に用いられたアルゴリズムに対応するので、相互認証が成功していれば、即ち、双方の機器で用いられるセキュア鍵が一致していれば、この復号によって得られるデータは、元の暗号化キー425に一致する。

【0106】なお、メモリカード109は、認証領域332へのアクセスコマンドの実行を終える度に、それに用いたセキュア鍵を破棄(消去)する。これによって、メモリカード109の認証領域332にアクセスする外部機器は、1個のコマンドを送出する度に、事前に相互認証を行い、それにパスしている必要がある。図17は、図16に示された相互認証における詳細な手順を示す通信シーケンス図である。ここでは、メモリカード109とプレーヤ201は、チャレンジ・レスポンス型の相互認証を行う。

【0107】メモリカード109は、プレーヤ201の正当性を検証するために、乱数を生成し、それをチャレンジデータとしてプレーヤ201に送る。プレーヤ201は、自己の正当性を証明するために、そのチャレンジデータを暗号化し、レスポンスデータとしてメモリカード109に返す。メモリカード109は、そのレスポンスデータと、チャレンジデータとして送った乱数を暗号化して得られる暗号化チャレンジデータとを比較し、一致している場合には、プレーヤ201の認証に成功した(OK)と認識し、そのプレーヤ201から送られてくる認証領域332へのアクセスコマンドを受け付ける。一方、比較の結果、一致しなかった場合には、認証に成功しなかった(NG)したと認識し、もし、その後プレーヤ201から認証領域332へのアクセスコマンドが送られてきたとしても、その実行を拒絶する。

【0108】同様にして、プレーヤ201は、メモリカード109の正当性を検証するために、上記認証と同様のやりとりを行う。つまり、乱数を生成し、それをチャレンジデータとしてメモリカード109に送る。メモリカード109は、自己の正当性を証明するために、そのチャレンジデータを暗号化し、レスポンスデータとしてプレーヤ201に返す。プレーヤ201は、そのレスポンスデータと、チャレンジデータとして送った乱数を暗号化して得られる暗号化チャレンジデータとを比較し、一致している場合には、メモリカード109の認証に成功した(OK)と認識し、そのメモリカード109の認証領域332へのアクセスコを行う。一方、比較の結果、一致しなかった場合には、認証に成功しなかった(NG)したと認識し、そのメモリカード109の認証領域332へのアクセスは断念する。

【0109】なお、これら相互認証における暗号化アルゴリズムは、メモリカード109及びプレーヤ201が正当な機器である限り、全て同一である。また、メモリ

カード109及びプレーヤ201は、それぞれの認証及び証明において生成した暗号化チャレンジデータとレスポンスデータとを排他的論理和演算し、得られた結果をセキュア鍵として、メモリカード109の認証領域332へのアクセスのために用いる。そうすることで、双方の機器109及び201が相互認証に成功した場合にのみ共通となり、かつ、時変のセキュア鍵を共有し合うことが可能となり、これによって、認証領域332にアクセスする条件として相互認証に成功していることが条件とされることになる。

【0110】なお、セキュア鍵の生成方法として、暗号化チャレンジデータとレスポンスデータとセキュアメディアIDとの排他的論理和をとることとしてもよい。次に、本メモリカード109の認証領域332と非認証領域331との境界線の変更機能についての変形例について、図18及び図19を用いて説明する。図18は、境界線を変更する前のフラッシュメモリ303の使用状態を示す図である。図18(a)は、フラッシュメモリ303の物理ブロックの構成を示すメモリマップである。

【0111】図18(b)は、非認証領域アクセス制御部326内の不揮発な記憶領域等に置かれる非認証領域331専用の変換テーブル1103であり、非認証領域331の論理ブロックと物理ブロックとの対応関係が格納されている。非認証領域アクセス制御部326は、この変換テーブル1103を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を越えるアクセス違反を検出することができる。

【0112】図18(c)は、認証領域アクセス制御部325内の不揮発な記憶領域等に置かれる認証領域332専用の変換テーブル1102であり、認証領域332の論理ブロックと物理ブロックとの対応関係が格納されている。認証領域アクセス制御部325は、この変換テーブル1102を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を越えるアクセス違反を検出することができる。

【0113】境界線の変更前においては、図18(a)に示されるように、フラッシュメモリ303の代替領域を除いた記憶領域(物理ブロック0000~EFFF)のうち、境界線よりも下位アドレスに位置する物理ブロック0000~DFFFが非認証領域331に割り当てられ、上位アドレスに位置する物理ブロックE000~EFFFが認証領域332に割り当てられている。

【0114】そして、図18(b)に示された変換テーブル1102から分かるように、非認証領域331においては、物理ブロックと論理ブロックの番号が一致するように対応づけられている。一方、図18(c)に示された変換テーブル1103から分かるように、認証領域332においては、物理ブロックと論理ブロックとは、その番号の並びが逆順になっている。つまり、論理ブロック0000~0FFFそれぞれが物理ブロックE F F

F~E000に対応している。これは、論理ブロックは昇順に使用されていくことと、境界線が移動された場合において領域変更の生じた物理ブロックのデータ退避や移動処理の手間を考慮したからである。

【0115】図19(a)~(c)は、境界線を変更した後のフラッシュメモリ303の使用状態を示す図であり、それぞれ、変更前の図18(a)~(c)に対応する。なお、境界線の変更は、そのアドレスを指定する専用のコマンドがコマンドピンからコマンド判定制御部322に入力されたときに、コマンド判定制御部322によって認証領域アクセス制御部325内の変換テーブル1102及び非認証領域331内の変換テーブル1103が書き換えられることにより、実現される。

【0116】図19(a)~(c)に示されるように、ここでは、物理ブロックE000とDFFF間に置かれていた境界線が物理ブロックD000とCFFF間に移動されている。つまり、非認証領域331のサイズを1000(hex)個だけ減少させ、認証領域332のサイズを1000(hex)だけ増加させている。それに伴って、図19(b)に示されるように、非認証領域331の変換テーブル1103のサイズは、1000(hex)個のエントリー分だけ減少され、その結果、論理ブロック0000~CFFFに対応する物理ブロック0000~CFFFが示されている。一方、図19(c)に示されるように、認証領域332の変換テーブル1102のサイズは、1000(hex)個のエントリー分だけ増加され、その結果、論理ブロック0000~1FFFに対応する物理ブロックEFFF~D000が示されている。

【0117】このように、フラッシュメモリ303の一定領域において境界線によって非認証領域と認証領域とを区切り、その境界線の移動によって各領域のサイズを変更することにより、このメモリカード109の多様な応用、例えば、保護すべきデジタル著作物の格納を主要な用途とする場合やその逆の場合等に対応させることが可能となる。

【0118】そして、非認証領域及び認証領域いずれにおいても、境界線に近いアドレスの物理ブロックから境界線に近いアドレスの物理ブロックに向かって、使用していくように論理ブロックと物理ブロックとを対応づけることで、境界線の移動に伴うデータ退避や移動処理等の手間が削減される。また、そのような対応づけは、認証領域332専用の変換テーブル1102と非認証領域331専用の変換テーブル1103とに分離して設けることで、その実現が容易となる。

【0119】なお、認証領域332においては、ブロックの単位で論理アドレスと物理アドレスとが逆順になっていたが、このような単位に限られず、例えば、セクタの単位で逆順としたり、バイトの単位で逆順としてもよい。以上、本発明のメモリカードについて、実施の形態

及び変形例を用いて説明したが、本発明はこれらに限定されるものではない。

【0120】例えば、PC102やプレーヤ201は、メモリカード109の認証領域332にアクセスするためのコマンドを発する度に同じ手順によるメモリカード109との認証が必要とされたが、コマンドの種類によっては簡略化された認証手順でアクセスできるようにしてもよい。例えば、書き込みコマンド「SecureWrite」については、メモリカード109から暗号化マスター鍵323bやメディアID341を取り出す必要はなく、片方向の認証（メモリカード109による機器の認証だけ）に成功するだけで、メモリカード109により実行されるとしてもよい。これによって、あまり著作権保護との関連が強くないコマンドについては、その実行速度が高速化される。

【0121】また、本発明のメモリカード109が有するフラッシュメモリ303を他の記憶メディア、例えば、ハードディスク、光ディスク、光磁気ディスク等の不揮発メディアに置き換えても本発明と同様の著作権保護が可能な携帯型記憶カードが実現されることは言うまでもない。

【0122】

【発明の効果】以上の説明から明らかなように、本発明に係る半導体メモリカードは、電子機器に着脱可能な半導体メモリカードであって、書き換え可能な不揮発メモリと、前記不揮発メモリ内の予め定められた2つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路と、前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備え、前記制御回路は、前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御部と、前記電子機器の正当性を検証するために前記電子機器の認証を試みる認証部と、前記認証部が認証に成功した場合にだけ前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御部とを有し、前記認証領域と前記非認証領域は、前記不揮発性メモリ内の一定サイズの連続した記憶領域を2分して得られる各領域に割り当てられ、前記領域サイズ変更回路は、前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、前記非認証領域における論理アドレスと物理アドレスとの対応を示す非認証領域変換テーブルと、前記電子機器からの命令に従って前記認証領域変換テーブル及び前記非認証領域変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を2分して得られる物理アドレ

スの高い領域及び低い領域に割り当てられ、前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられていることを特徴とする。

【0123】これにより、著作権保護に関わるデータを認証領域に格納し、そうでないデータを非認証領域に格納することで、デジタル著作物と非著作物とを混在させて使用することができ、両方の用途を兼ね備えた半導体メモリカードが実現される。前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられているので、論理アドレスの昇順に使用していくことにより、認証領域と非認証領域との境界付近の領域が使用される確率が低くなる。故に、その境界を移動させた場合に必要とされるデータ退避や移動等の処理が発生する確率も低くなり、領域サイズの変更が簡単化される。

【0124】前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御するので、同一ファイルを構成する複数の論理ブロックが断片化する現象が生じても、論理的に連続した論理ブロックとなるように容易に変更することができるので、同一ファイルへのアクセスが高速化される。

【0125】ここで、前記認証部は、認証の結果を反映した鍵データを生成し、前記認証領域アクセス制御部は、前記電子機器から送られてくる暗号化された命令を前記認証部が生成した鍵データで復号し、復号された命令に従って前記認証領域へのアクセスを制御するとしてもよい。これによって、半導体メモリカードと電子機器とのやりとりが盗聴されたとしても、認証領域にアクセスするための命令は、直前に行われた認証結果に依存して暗号化されているので、認証領域への不正なアクセスに対する防止機能が高くなる。

【0126】また、前記認証部は、前記電子機器とチャレンジ・レスポンス型の相互認証を行い、前記電子機器の正当性を検証するために前記電子機器に送信したチャレンジデータと自己の正当性を証明するために生成したレスポンスデータとから前記鍵データを生成するとしてもよい。これによって、鍵データは、半導体メモリカードと電子機器の双方が相互認証に成功したときのみ初めて双方において共有され、かつ、認証の度に変化するという性質を有するので、そのような鍵データを用いなければアクセスすることができない認証領域の安全性はより強いものとなる。

【0127】また、前記電子機器から送られてくる暗号化された命令は、前記認証領域へのアクセスの種別を特定する暗号化されていないタグ部と、アクセスする領域を特定する暗号化されたアドレス部とからなり、前記認証部は、前記鍵データを用いて、前記命令のアドレス部を復号し、復号されたアドレスによって特定される領域に対して、前記命令のタグ部によって特定される種別のアクセスを実行制御するとしてもよい。

【0128】これによって、命令のアドレス部だけが暗号化されるので、このような命令を受け取った半導体メモリカードでの復号や解読処理は簡易となる。また、前記半導体メモリカードはさらに、他の半導体メモリカードと区別して自己を特定することが可能な固有の識別データを予め記憶する識別データ記憶回路を備え、前記認証部は、前記識別データ記憶回路に格納された識別データを用いて相互認証を行い、前記識別データに依存させて前記鍵データを生成するとしてもよい。

【0129】これによって、相互認証においては、個々の半導体メモリカードに依存したデータが交換されるので、不正な相互認証の解読に対して高い安全性を維持することができる。また、前記半導体メモリカードはさらに、予めデータが格納された読み出し専用のメモリ回路を備えてもよい。これによって、他の半導体メモリカードと区別できる識別データ等を読み出し専用メモリに格納し、デジタル著作物をその識別データに依存させて格納したりすることで、著作権保護の機能が強化される。

【0130】また前記認証領域及び前記非認証領域は、前記電子機器にとって読み書き可能な記憶領域と読み出し専用の記憶領域とからなり、前記制御回路はさらに、前記電子機器が前記不揮発メモリにデータを書き込むためのアクセスをする度に乱数を発生する乱数発生器を有し、前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記乱数を用いて前記データを暗号化し、得られた暗号化データを前記読み書き可能な記憶領域に書き込むとともに、前記乱数を前記暗号化データに対応づけられた前記読み出し専用の記憶領域に書き込むとしてもよい。

【0131】これによって、読み書き可能な記憶領域に対する不正な改ざん等が行われても、読み出し専用の記憶領域に格納された乱数との整合性を検査することで、そのような行為を検出することが可能となるので、より安全なデータ記録が実現される。前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有してもよい。これによって、半導体メモリカードを破壊して認証領域及び非認証領域のメモリ内容を直接読み出す等の不正な攻撃に耐えることが可能となる。

【0132】また、前記不揮発メモリは、フラッシュメモリであり、前記制御回路はさらに、前記電子機器から

の命令に従って、前記認証領域及び前記認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有してもよい。これによって、電子機器は、フラッシュメモリの書き換えに先立って、未消去の領域を知り、その領域を事前に消去しておくことができるので、高速な書き換えが可能となる。

【0133】また、前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、前記制御回路はさらに、前記ユーザキーを記憶しておくためのユーザキー記憶部と、前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有してもよい。

【0134】これによって、半導体メモリカードと接続して使用する度にパスワードや個人データの入力が要求されるという手間が回避されるので、不正に個人データが盗聴されて利用されるという不具合の発生が抑えられる。本発明に係る読み出し装置は、上記半導体メモリカードに格納されたデジタル著作物を読み出す読み出し装置であって、前記半導体メモリカードは、非認証領域に、デジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の読み出しを許可する回数が予め格納され、前記読み出し装置は、前記非認証領域に格納されたデジタル著作物を読み出す際に、前記認証領域に格納された回数を読み出し、その回数によって読み出しが許可されているか否か判断する判断手段と、許可されている場合にのみ前記非認証領域から前記デジタル著作物を読み出すとともに、読み出した前記回数を減算して前記認証領域に書き戻す再生手段とを備えることを特徴とする。

【0135】これによって、半導体メモリカードに格納されたデジタル著作物の読み出し回数を制限することが可能となり、音楽コンテンツの有料レンタル等への適用が可能となる。また、本発明に係る読み出し装置は、上記半導体メモリカードに格納されたデジタル著作物を読み出してアナログ信号に再生する読み出し装置であって、前記半導体メモリカードは、非認証領域に、アナログ信号に再生可能なデジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の前記電子機器によるデジタル出力を許可する回数が予め格納され、前記読み出し装置は、前記非認証領域に格納されたデジタル著作物を読み出してアナログ信号に再生する再生手段と、前記認証領域に格納された回数を読み出し、その回数によってデジタル出力が許可されているか否か判断

する判断手段と、許可されている場合にのみ前記デジタル著作物をデジタル信号のまま外部に出力するとともに、読み出した前記回数を減算して前記認証領域に書き戻すデジタル出力手段とを備えることを特徴とする。

【0136】これによって、半導体メモリカードに格納されたデジタル著作物のデジタルコピーの回数を制限することが可能となり、著作権者の意図に沿った木目の細かい著作権保護が可能となる。このように、本発明は、デジタル著作物の記録媒体としての用途とコンピュータの補助記憶装置としての用途の両方を兼ね備えた柔軟な機能

【図面の簡単な説明】

【図1】本発明の実施の形態における電子音楽配信に係るパソコンと、そのPCに着脱可能な半導体メモリカードの外観を示す図である。

【図2】同半導体メモリカードを記録媒体とする携帯型のプレーヤの外観を示す図である。

【図3】同パソコンのハードウェア構成を示すブロック図である。

【図4】同プレーヤのハードウェア構成を示すブロック図である。

【図5】同半導体メモリカードの外観及びハードウェア構成を示す図である。

【図6】同パソコンや同プレーヤから見た同半導体メモリカードの記憶領域の種類を示す図である。

【図7】同パソコンや同プレーヤが同半導体メモリカードの各領域にアクセスする際の制限やコマンドの形態を示す図であり、(a)は各領域へのアクセスにおけるルールを示し、(b)は各領域のサイズの変更におけるルールを示し、(c)は同半導体メモリカードの領域を示す概念図である。

【図8】音楽データ等のコンテンツを同パソコン(及び同プレーヤ)が同半導体メモリカードに書き込む動作を示すフロー図である。

【図9】音楽データ等のコンテンツを同半導体メモリカードから読み出して同プレーヤ(及び同パソコン)で再生する動作を示すフロー図である。

【図10】同プレーヤ(及び同パソコン)が同半導体メモリカードの認証領域に格納された読み出し回数を操作する動作を示すフロー図である。

【図11】同プレーヤ(及び同パソコン)が同半導体メモリカードの認証領域に格納されたデジタル出力許可回数を操作する動作を示すフロー図である。

【図12】同半導体メモリカードの認証領域及び非認証領域に共通のデータ構造と、そのデータ構造に対応した読み書き処理のフローとを示す図である。

【図13】同半導体メモリカードの論理アドレスと物理アドレスとの対応を変更する様子を示す図であり、

(a)は変更前の対応関係、(b)は変更後の対応関係、(c)は(a)に対応する変換テーブル、(d)は(b)に対応する変換テーブルを示す。

【図14】同半導体メモリカードが有する未消去ブロックに関する機能を説明する図であり、(a)は論理ブロック及び物理ブロックの使用状態を示し、(b)はその状態における未消去リストを示し、(c)はPC102やプレーヤ201が未消去リストコマンドと消去コマンドを用いて事前にブロックを消去する場合の動作を示すフロー図であり、(d)は論理ブロックの使用状態を示すテーブルである。

【図15】認証のための同プレーヤと同半導体メモリカード間の通信シーケンス及び主要な構成要素を示す図である。

【図16】本発明の変形例に係る同半導体メモリカードと外部機器との認証手順を示す通信シーケンス図である。

【図17】図16に示された相互認証の詳細な手順を示す通信シーケンス図である。

【図18】同半導体メモリカードの認証領域と非認証領域との境界線の変更における変更前の状態を示す図であり、(a)はフラッシュメモリの物理ブロックの構成を示すメモリマップであり、(b)は非認証領域専用の変換テーブルを示し、(c)は認証領域専用の変換テーブルを示す。

【図19】同半導体メモリカードの認証領域と非認証領域との境界線の変更における変更後の状態を示す図であり、(a)はフラッシュメモリの物理ブロックの構成を示すメモリマップであり、(b)は非認証領域専用の変換テーブルを示し、(c)は認証領域専用の変換テーブルを示す。

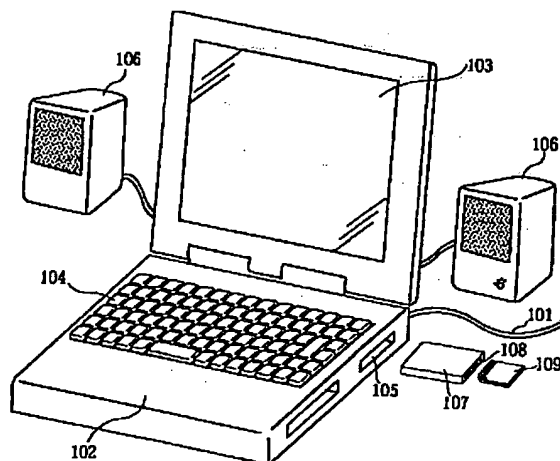
【符号の説明】

| | |
|-----|--------------|
| 101 | 通信回線 |
| 102 | PC |
| 103 | ディスプレイ |
| 104 | キーボード |
| 105 | メモリカードライタ挿入口 |
| 106 | スピーカ |
| 107 | メモリカードドライタ |
| 108 | メモリカード挿入口 |
| 109 | メモリカード |
| 110 | CPU |
| 111 | ROM |
| 112 | RAM |
| 113 | 通信ポート |
| 114 | 内部バス |
| 117 | デスクランブラ |
| 118 | AACデコーダ |
| 119 | D/Aコンバータ |
| 120 | ハードディスク |

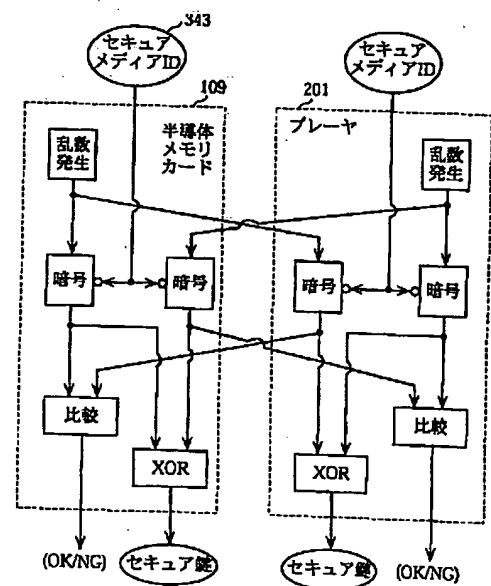
201 プレーヤ
 202 操作ボタン
 203 液晶表示部
 204 アナログ出力端子
 205 デジタル出力端子
 206 メモリカード挿入口
 208 ヘッドフォン
 210 CPU
 211 ROM
 212 RAM
 213 通信ポート
 214 内部バス
 215 カードI/F部
 216 認証回路
 217 ディスクランブラ
 218 AACデコーダ
 219 D/Aコンバータ
 220 AACエンコーダ
 221 A/Dコンバータ
 222 スランブラ
 223 アナログ入力端子
 224 スピーカ
 302 コントロールIC
 303 フラッシュメモリ
 304 ROM (特殊領域)
 321 認証部
 322 コマンド判定制御部
 323 マスター鍵記憶部
 323a マスター鍵

* 323b 暗号化マスター鍵
 324 特殊領域アクセス制御部
 325 認証領域アクセス制御部
 326 非認証領域アクセス制御部
 327 暗号・復号化回路
 331 非認証領域
 332 認証領域
 341 メディアID
 342 製造メーカー名
 343 セキュアメディアID
 425 暗号化キー
 426 暗号化コンテンツ
 427 ユーザデータ
 501 代替ブロック領域
 812 読み出し回数
 913 デジタル出力許可回数
 1003 乱数発生器
 1004 セクタ
 1005 拡張領域
 1006 ECCデータ
 1007 時変領域
 1101 変換テーブル
 1102 認証領域専用変換テーブル
 1103 非認証領域専用変換テーブル
 1203 未消去リスト
 1301 マスター鍵
 1302 機器固有ID
 1310 機器固有ID群記憶領域
 * 1311 ユーザキー記憶領域

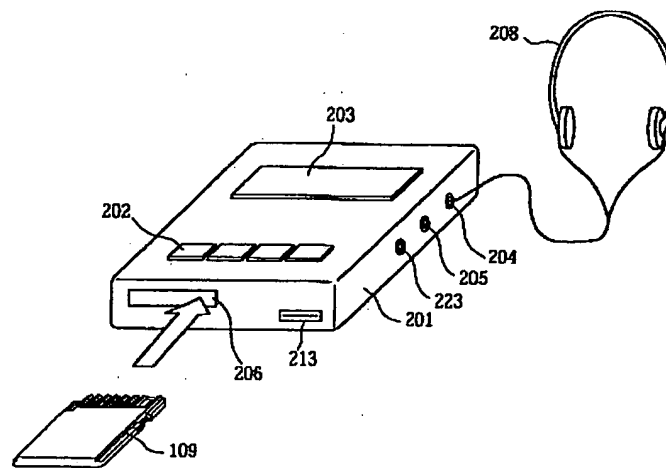
【図1】



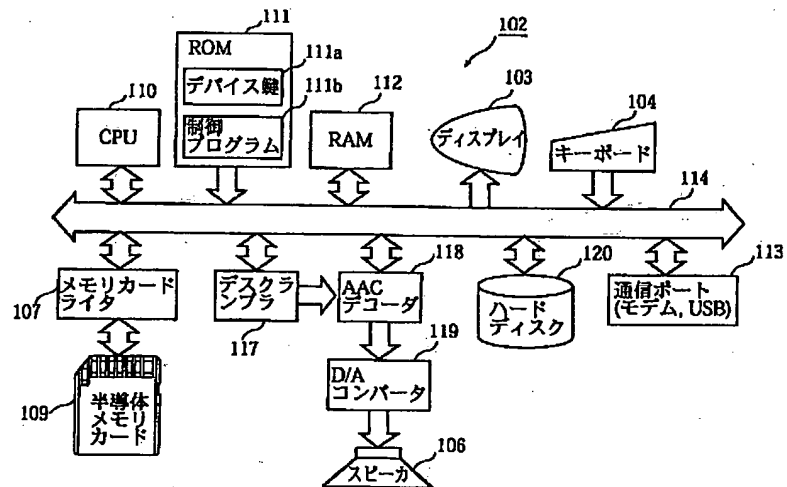
【図17】



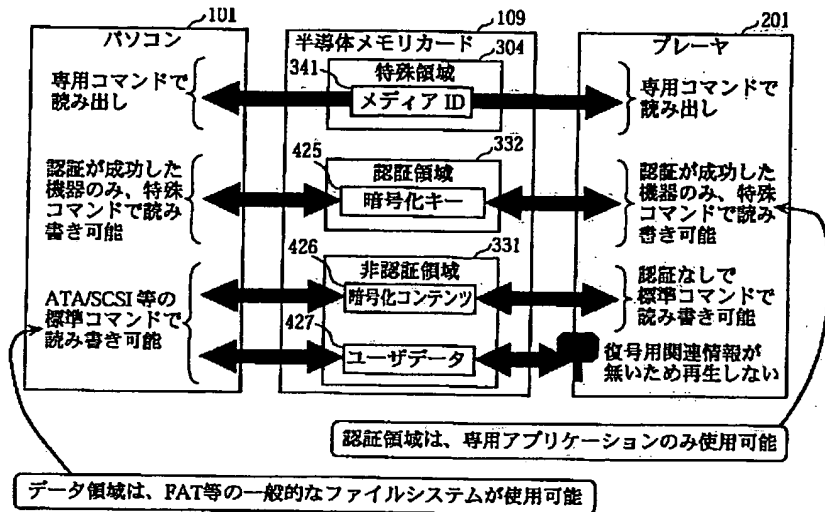
【図2】



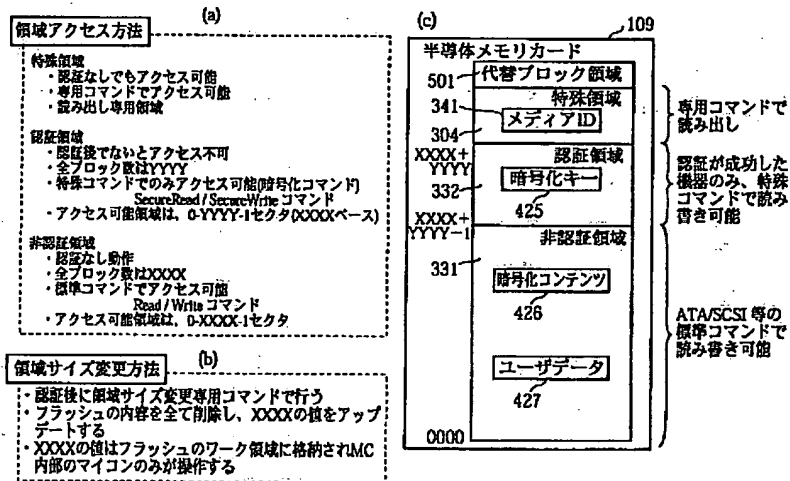
【図3】



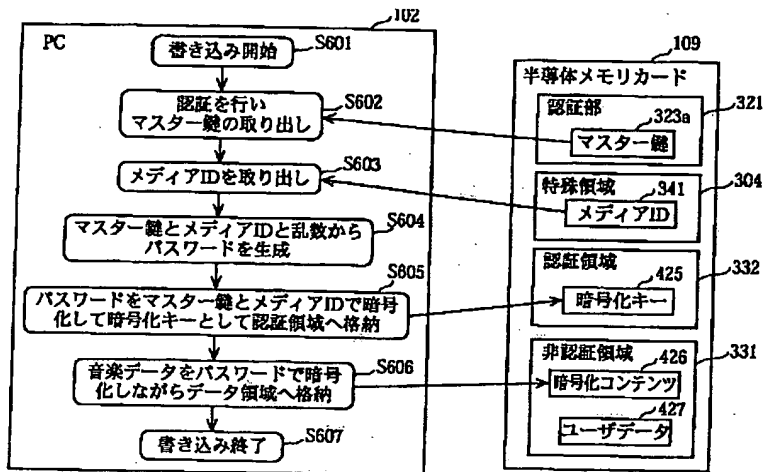
【図6】



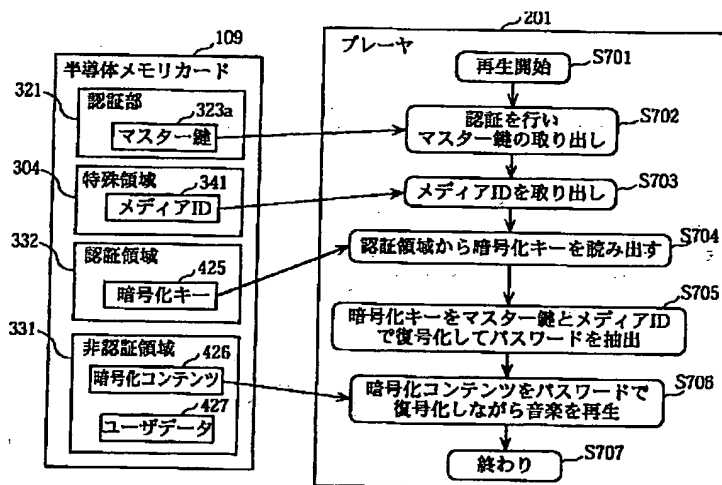
【図7】



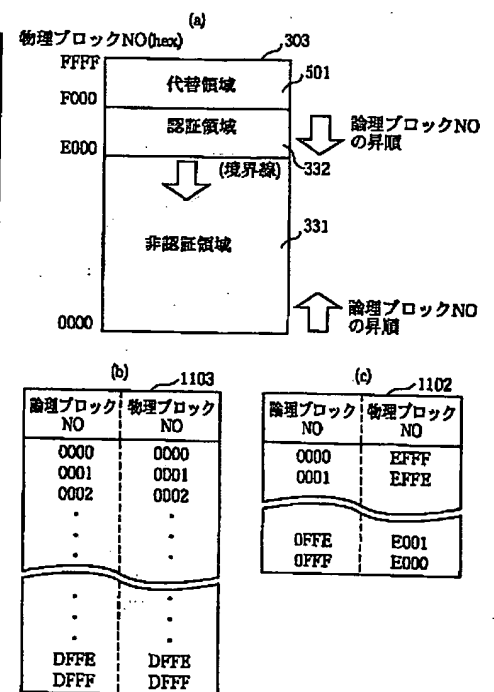
【図8】



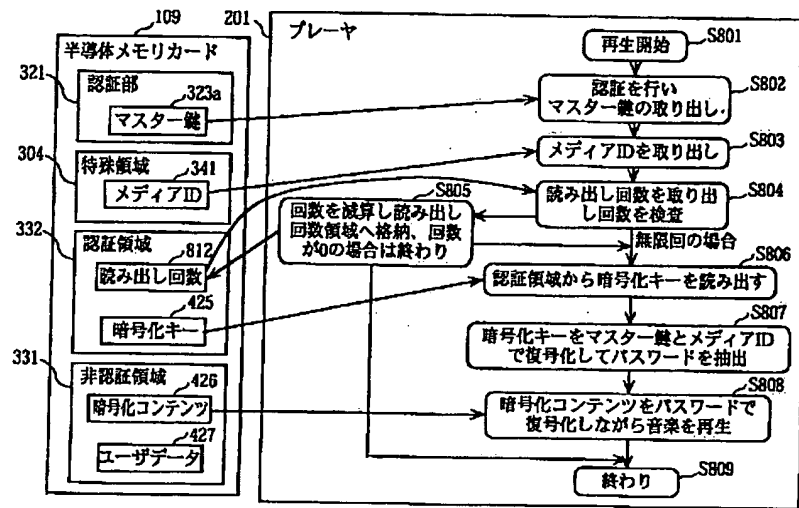
【図9】



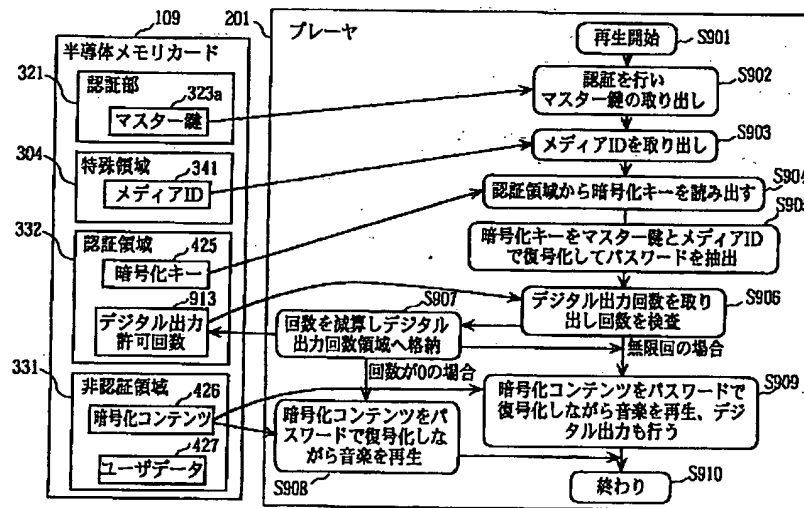
【図18】



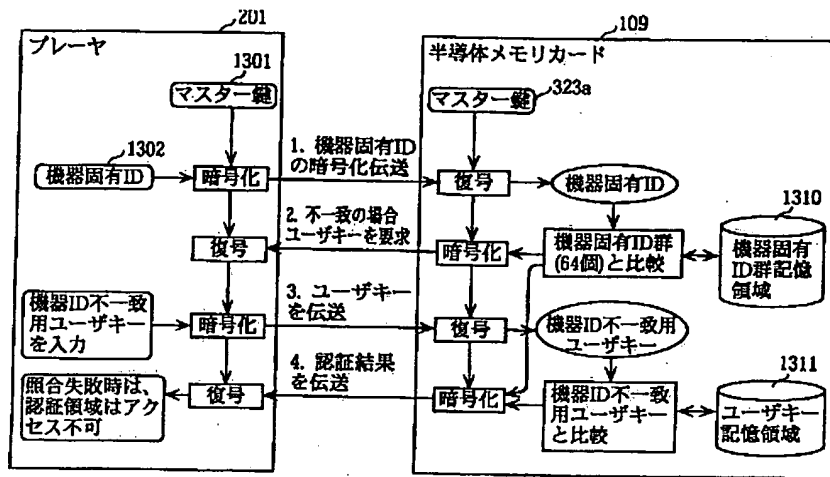
【図10】



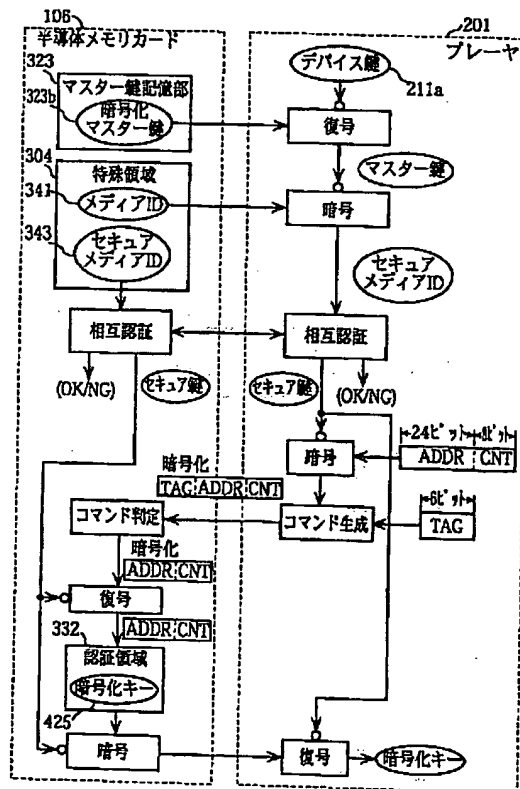
【図11】



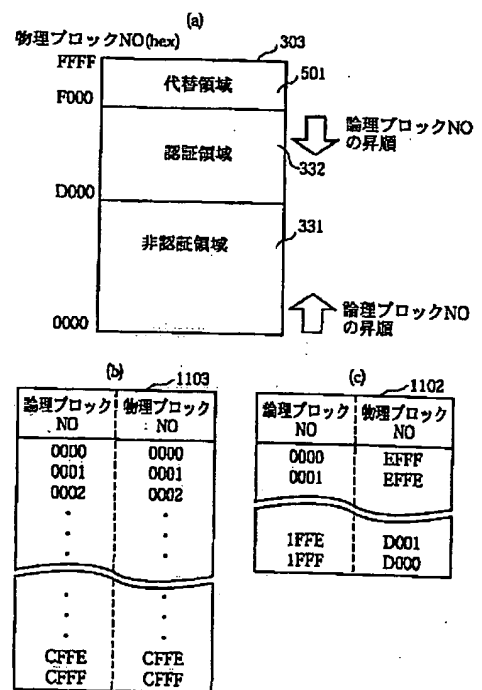
【図15】



【図16】



【図19】



フロントページの続き

(51) Int. Cl.

G 0 9 C 1/00

識別記号

6 4 0

6 6 0

F I

G 0 9 C 1/00

G 0 6 K 19/00

テーマコード(参考)

6 6 0 A

R

H04L 9/32

H04L 9/00

675A

(72)発明者 湯川 泰平
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 南 賢尚
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 小塚 雅之
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
Fターム(参考) 5B017 AA03 AA06 BA01 BA07 BB10
CA14
5B035 AA13 BB09 BB11 CA11 CA29
5B058 CA02 CA23 CA24 CA25 KA01
KA02 KA04 KA06 KA12 KA31
KA35
5J104 AA07 DA02 KA02 NA35